Oppfølging av SIL i drift

Oppdatering av feilrater og testintervaller

Praktiske erfaringer fra driftsgjennomganger hos ulike operatører

Solfrid Håbrekke, SINTEF Teknologi og samfunn, avd. Sikkerhet

solfrid.habrekke@sintef.no

Innhold

- Hva er **hensikten** med operasjonelle driftsgjennomganger?
- Gjennomføringer av **operasjonelle driftsgjennomganger**
- **Resultater og funn** fra gjennomganger
- **PDS Tool** for oppfølging av instrumenterte sikkerhetssystemer i drift

Hva er hensikten med operasjonell driftsgjennomgang?

- Ptil-krav om oppfølging av barrierer

- Selskapets egne krav til oppfølging
- Systematisering av vedlikeholdsdata
- Oversikt over sikkerhetssystemene
- Oppdaterte feilrater
- Endre testintervaller
- Identifisering av:
  - Typiske feil
  - Fellesfeil
  - Forbedringsområder
  - …

- Tilbakemelding til leverandører på utstyr

- Generiske feilrater (PDS)

PETROLEUMSTILSYNET

SINTEF

Verifisere ytelseskrav og opprettholde sikkerheten

Operasjonell driftsgjennomganger i praksis

- Alle sikkerhetsfunksjoner med SIL krav skal følges opp. Et anlegg består ofte av flere hundre ulike looper / sikkerhetsfunksjoner. Har man kontroll med hver enkelt utstyrsgruppe kan man anta å ha kontroll med totalen.

- Verifisere antagelser fra design i driftsfasen
  - Feilrater
  - Testintervaller
  - …

- Forbedre detaljert feilrapportering og klassifisering av feil

- Anbefalt gjennomført årlig

Operasjonell driftsgjennomganger i praksis forts.

- Utstyrsgrupper
- Notifikasjoner
  - Klassifisering
  - Verifisering
- Kommunikasjon mellom vedlikeholdsmiljøet og instrument/automasjon/teknisk sikkerhet
- Gjennomgangen dokumenteres i rapport

Datainnsamling ved operasjonell driftsgjennomgang

- For hver notifikasjon:
  - Er feilen **Dangerous** (**D**) eller **Safe** (**S**)**?**
  - Deteksjonsmåte: **Detektert** (**D**) eller **Udetektert** (**U**) ?
    - Detektert: Alarm/diagnostikk, overvåking, osv. – λ_{DD}
    - Udetektert: Test, ved behov, tilfeldig, osv. – λ_{DU}
  - Hva var årsaken?

- For hver utstyrsgruppe:
  - Aggregert driftstid (dvs. antall komponenter i hver utstyrsgruppe og operasjonstid)
  - Gjeldende testintervall
  - Antatt feilrate fra design

Kvantitativ analyse – oppdatering av feilrater og testintervall

- Ser bort fra burn-in failures…
- Tar hensyn til operasjonell driftstid
- Sammenligner med target (basert på forventet antall feil i perioden gitt antatt feilrate) – Må kompenserende tiltak implementeres?

- Merk at komponentene må ha vært aktivert (demand eller test) minst én gang i løpet av observasjonsperioden!

$$\hat{\lambda}_{DU} = \frac{\text{Antall DU}-\text{feil}}{\text{Observasjonstid}}$$

- Kvalitativ vurdering av evt. forslag til nytt testintervall

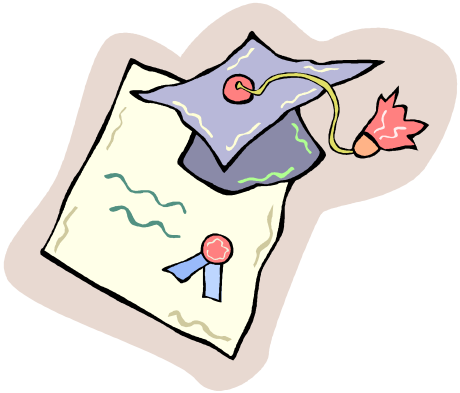
Kvalitativ analyse

- Praktiske konsekvenser for endring av testintervall; er det praktisk mulig mht. vedlikeholdsrutiner og vedlikeholdskampanjer å endre testintervallene?
- Leverandøranbefalinger; hva anbefaler og antar leverandøren mht. testing?
- Kvaliteten i feildataene; er alle relevante feil samla inn og riktig klassifisert?
- Relevans i forhold til utstyret; er data samla inn for utstyr som er skifta ut eller utstyr som fremdeles er i drift?
- Kvalitet på testing; er alle potensielle DU-feil avdekka av dagens prosedyrer?
- Skyldes feilene samme årsak/fellesfeil?
- Sekundæreffekter av testing; vil hyppigere testing introdusere nye feil eller vil sjeldnere testing fører til at komponenter vil slites før neste test?

Resultater fra en operasjonell driftsgjennomgang

- Oppdaterte feilrater
- Oppdaterte testintervaller. Testintervall har kunnet blitt justert for mange utstyrsgrupper
- Nyttig for operatøren og vedlikeholdspersonell å få "totaloversikt"
- Se på trender fra år til år
- Avdekke spesielle problemer, repeterende feil, mulige fellesfeil, osv.
- Økende kvalitet på notifikasjoner og bedre rutiner for feilrapportering
- Avdekke svakheter ved vedlikeholdsstrategi
- Forbedret kvalitet på testprosedyrer
- Forbedret rapportering i vedlikeholdssystemet

- Har man gjort det en gang, vil man fortsette...



Eksempel - ESD/PSD ventiler

- Totalt 162 DU-feil

- Feilmoder:
  - 52% Delayed Operation
  - 39% Fail to Close on demand
  - 7% Leakage in Closed Position
  - 3% Fail to Open on demand (Gjelder fail-open ventiler)

- Årsaker:
  - 44% med ukjent årsak
  - Mest vanlige årsaker:
    - Feil med aktuator
    - Hydraulikkproblem
    - Frosset/Is
    - Treghet
    - Rust
    - Skitt
    - Avbløding (CCF)
  - Noen få årsaker er registrert for flere installasjoner, men de fleste kun for én installasjon

Tiltak etter en operasjonell driftsgjennomgang

- Endre testintervaller
- Behov for mer intensivt vedlikehold (hvis for høye feilrater)
- Utbedre testprosedyrer for å avdekke flere typer feil
- Vurdere utskifting til mer tilpasset utstyr
- Kursing av personell
- Forbedre rutiner og prosedyrer
- Forbedre årsaksanalyse

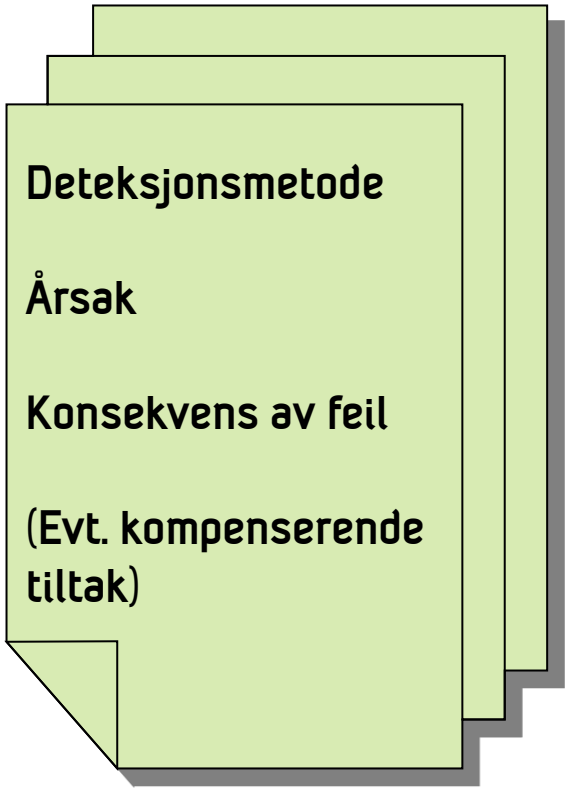
- Tiltakene må sjekkes mot SAR/SRS/QRA/SIL compliance document og anbefalinger i disse

Viktigste forbedringsområder fra gjennomganger

- Enda bedre kvalitet på notifikasjoner.
  - Klassifisering av feil – Har konsekvenser for prioritering og rapportering
  - Feil oppdaget ved test vs. feil i drift
  - Manglende årsaksanalyse

Kvalitet på notifikasjoner

- Stor variasjon i beskrivelsene
- Opp til flere feil skrevet på samme notifikasjon
- Utstyr som mangler tag havner i "tilfeldige" utstyrsgrupper
  - Logikk, barrierer, endebrytere, kontrollsystem
- Manglende informasjon
  - Gangtid på stengeventiler
  - Åpningstrykk for PSVer
  - Alarmer transmittere
- Feil klassifisering av feilmode, deteksjonsmetode, osv.
  - Behov for opplæring av operatører som fyller ut vedlikeholdsnotifikasjoner.



- MEN generelt mye informasjon (om man "leiter")

Klassifisering av feil – Prioritering av vedlikehold

- Feilklassifiserte notifikasjoner mht. deteksjonsmetode, feilmode, osv.
- Prioritering av oppretting av feil er til dels avhengig av klassifisering av bl.a. feilkode og alvorlighet av feil. Anvendte koder ikke alltid lett å forstå.
- Feil klassifisering kan føre til at en kritisk feil blir liggende lengre enn den burde (uten kompenserende tiltak)

  -> Høyere utilgjengelighet -> dårligere PFD -> SIL krav ikke tilfredsstilt

- **Bør etableres en tydelig kobling mellom SIL krav og den kritikaliteten/prioriteringen til utstyr**

Klassifisering av feil – Feil oppdaget ved test versus feil oppdaget i drift

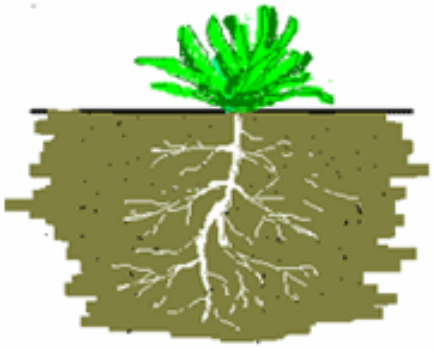
- For noe utstyr er test dominerende demand og de fleste DU-feil oppdages ved test (f.eks. B&G detektorer)
- For noe utstyr er "normal bruk" dominerende demand og de fleste DU-feil oppdages ved normal bruk (f.eks. branndører)
- Viktig å ta med feil oppdaget både ved test og "normal bruk". Dette er i henhold til IEC 61508/61511 og myndighetskrav om å ha kontroll på anlegget og helheten.
- **For å dekke helheten bør feil avdekket både ved test og i drift inkluderes**
- **Merk at rapportering til RNNP kun baserer seg på feil oppdaget ved test**

Årsaksanalyse?

SKR rapporterer at det er feilmelding på detektoren. Vi har etter beste evne forsøkt å sjekke om siktlinjen kan være blokkert av stillas. Det ser ikke slik ut, men nøyaktig måleutstyr kan kanskje gi et annet svar. Innfestingen er temmelig lealaus samtidig som den er plassert utsatt til. Dermed kan detektoren ha kommet ut av stilling. En tredje mulighet er at ektefellen ("receiveren") ikke vil kommunisere. Dette er et velkjent problem som rammer mange i dagens samfunn…

- **Repeterende feil** / problemkomponenter feiler gjerne mange ganger før man finner rotårsaken.
- Tar lang tid før reparasjon utføres – Hva med kompenserende tiltak?
- Fellesfeil oppdages seint

- **Rotårsaksanalyse** ☺



Hvorfor bedre notifikasjoner?

- Verktøy og tilnærminger som kun baserer seg på automatisk rapporterte data ikke nok
- En grad av manuell kvalitetssikring er viktig, også dersom en ønsker å avdekke bakenforliggende årsaker for utarbeidelse av forbedringstiltak.
- Mye feilrapportering fordi de anvendte kodene er vanskelig å forstå. Dette gjelder spesielt "failure impact", "detection method" og "failure mode".
- Må ofte "dykke dypt" samt diskutere med fagfolk for å klassifisere feil.
- Redusere repeterende feil
- Avdekke fellesfeil

- **Redusere samlet utilgjengelighet -> Opprettholde SIL-nivået**

Øvrige observasjoner fra driftsgjennomganger

- **Feil som blir liggende** uten å bli reparert (f.eks. detektorer) eller utstyr som blir liggende lenge med feil i påvente av nytt utstyr pga. lang leveringstid (typisk ventiler).
- Utstyr **ikke klassifisert som sikkerhetskritisk**
- **Feil rapportert mot "tilfeldig"/feil tag** (solenoider, I/O kort, barrierer, endebrytere, transmittere, logikk, osv.) og får ikke konsistent oppfølging
- En del utstyr er **eksponert for åpne/værutsatte områder**
- Høy andel **systematiske feil** (inkludert fellesfeil), dvs. designrelaterte feil samt feil som kan tilskrives bruk og vedlikehold av utstyret. Dette står i kontrast til de lave feilratene som ofte legges til grunn i designfasen (jf. sertifikatdata)

Øvrige observasjoner og funn fra driftsgjennomganger forts.

- Utstyr/funksjoner som er **vanskelig å teste** (f. eks. høyt nivå i lagertanker hvor man ikke våger å utsette tanken for dette nivået) eller har **vanskelig tilkomst** (f. eks. gassdetektorer som er plassert så høyt at en må ha stillas eller lift for å få testet dem)

- **Utstyr testes under forhold forskjellig fra normal drift** (f.eks. trykkløs prosess)

- **Utfordrende å teste hele funksjonen.** F.eks. pga. at man vil unngå nedstengninger, uheldig plassering/tilkomst av utstyr, fokus på testing av definert sikkerhetskritisk utstyr (detektorer, transmittere og ventiler) som medfører at diverse mindre utstyr ikke blir testet.

- Kunne vært flere **tilbakemeldinger mellom operatør og leverandør**

PDS – Pålitelighet av instrumenterte sikkerhetssystemer

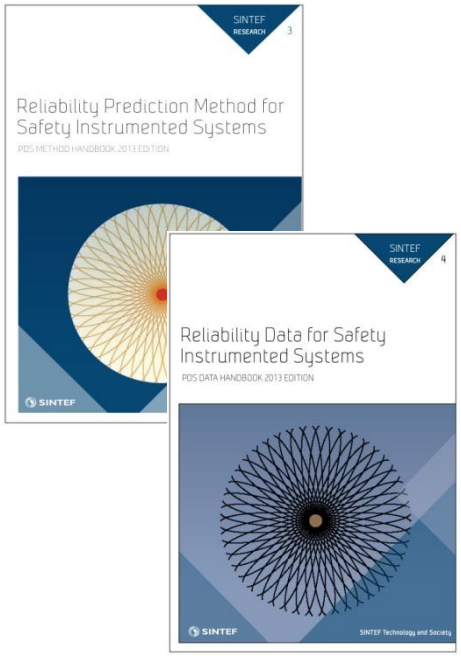
PDS forum

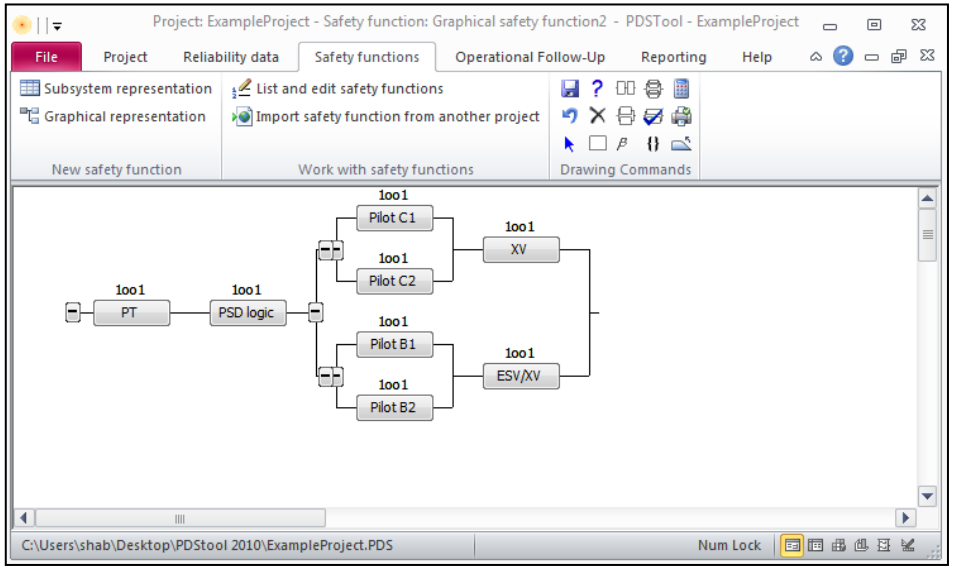
PDS metoden

PDS håndbøker

PDS rapporter

PDS Tool



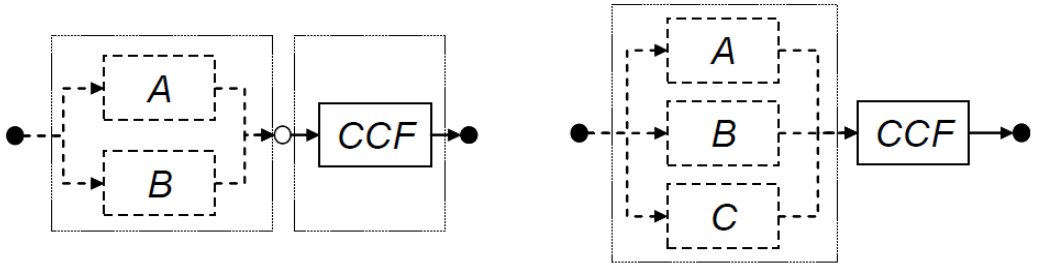


www.sintef.no/pds

ABB · origo · BP · ConocoPhillips · Eni Norge · FMC · GDF SUEZ · Honeywell · KONGSBERG · SAFETEC · Shell · Lilleaker Consulting a.s. · TOTAL · SIEMENS · DNV · TEEKAY CORPORATION · Statoil · SCANDPOWER Risk Management · A member of the Lloyd's Register Group · AkerSolutions · SIMTRONICS group · TALISMAN ENERGY · MARATHON · ODFJELL DRILLING

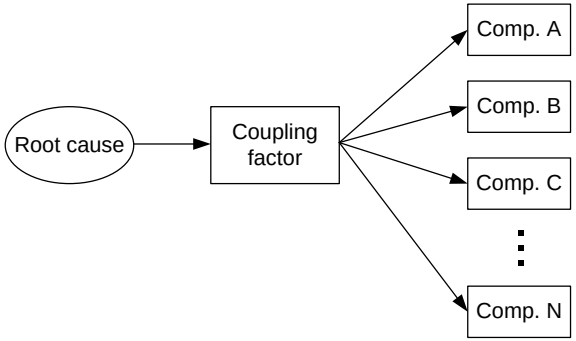
SINTEF · The Research Council of Norway · NTNU – Trondheim Norwegian University of Science and Technology

Fellesfeil

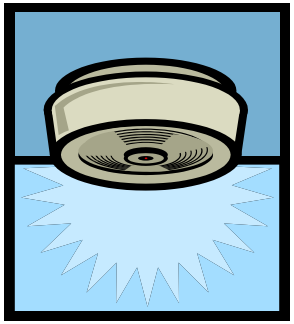


- *Failures of different items, resulting from a single event, where these failures are not consequences of each other* (ISO/DTR 12489)
- Feilene opptrer innenfor korteret tidsintervall (f.eks. et testintervall)

- Som en del av PDS forskningsprosjekt vil driftsgjennomgangen ha ekstra fokus på fellesfeil og identifisering av:
  - Årsak (**rotårsak**) til fellesfeil
  - Eventuelle **koblingsmekanismer** mellom komponenter (i samme utstyrsgruppe)

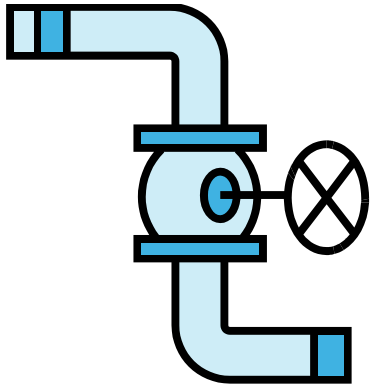


Typiske eksempler på fellesfeil – Detektorer og transmittere



- Linjedetektorer som ikke detekterer pga. snø eller stillas i siktelinje. *"Det er merkelig at det skal komme inn så mange alarmer akkurat mellom 8 og 16".*
- Feil plassering av detektorer (så de ikke detekterer når de skal)
- Skitne linser på detektorer plassert i eksponerte områder
- Programvarefeil (f.eks. tag som viser feil lokasjon av detektor i SKR)
- Kallibreringsfeil av transmittere (feil nivå eller feil medium)
- Transmittere som ikke er tilpasset medium (f.eks. nivåtransmittere for tanker med skum)

Typiske eksempler på fellesfeil – Ventiler



- Ventiler som ikke åpner/lukker på grunn av at de står i et forurenset eller rustutsatt område
- Vedlikeholdsrutiner som ikke sjekker hele funksjonaliteten til komponentene
- Ventiler som ikke fungerer pga. isdannelse (ikke tilstrekkelig isolasjon)
- Ventiler ikke designet for faktisk operasjonelt trykk
- For lang lukketid/åpningstid (f.eks. pga. feil med strupeventil, utilstrekkelig kapasitet, lekkasje i akkumulatorer, osv.)

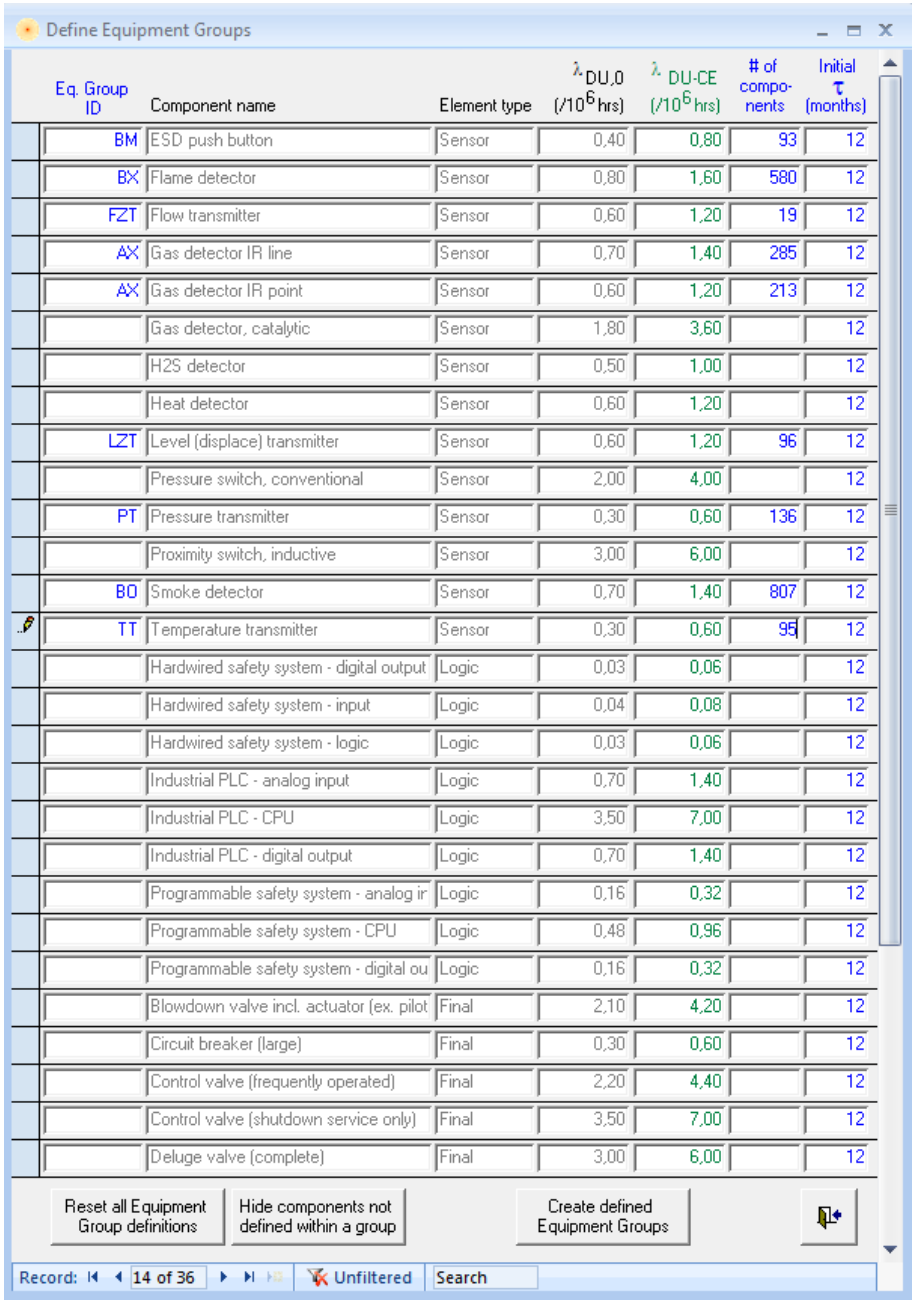
Eksempel - ESD/PSD ventiler

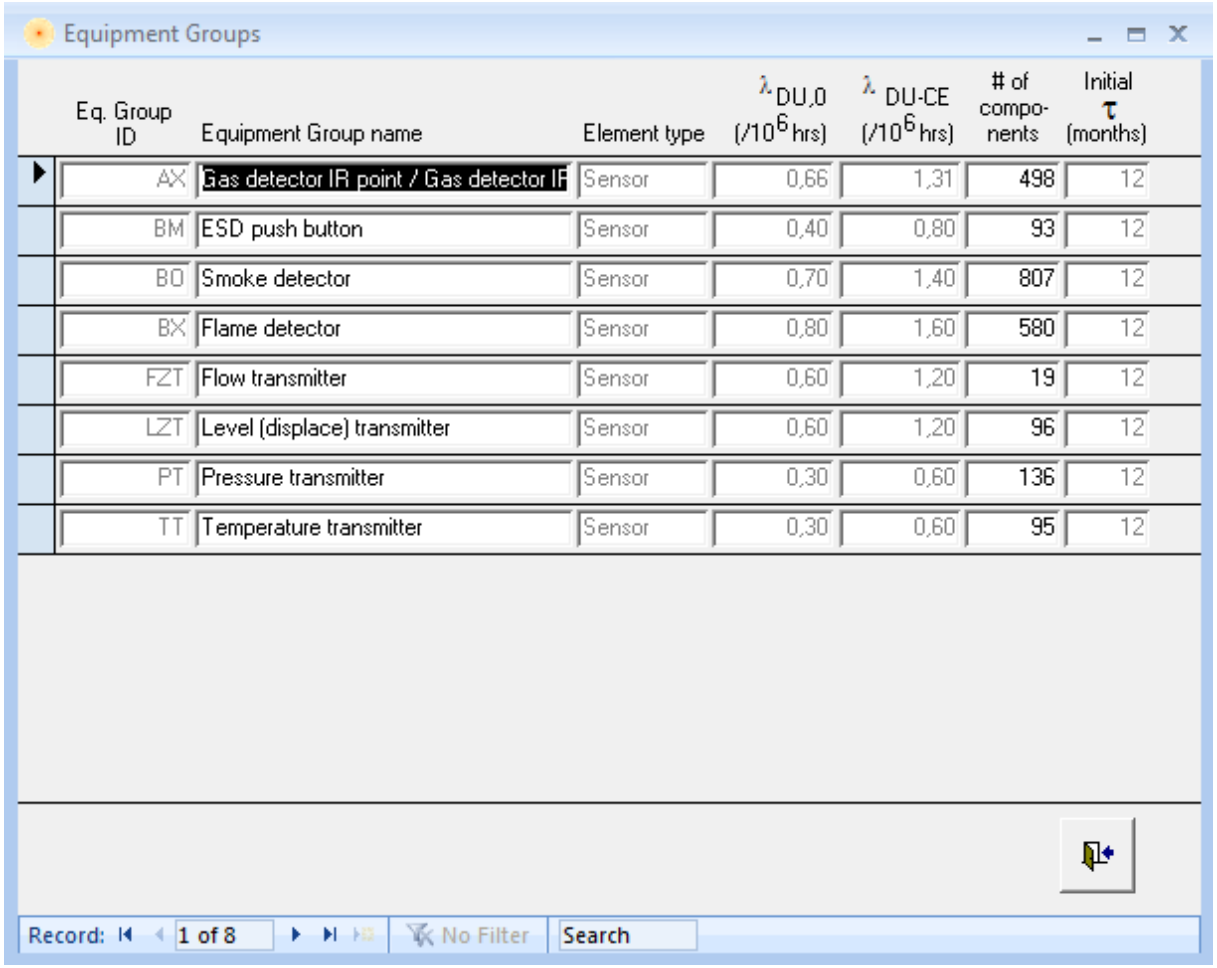
- 21% av DU-feilene er identifisert som fellesfeil, men kan være flere potensielle fellesfeil…

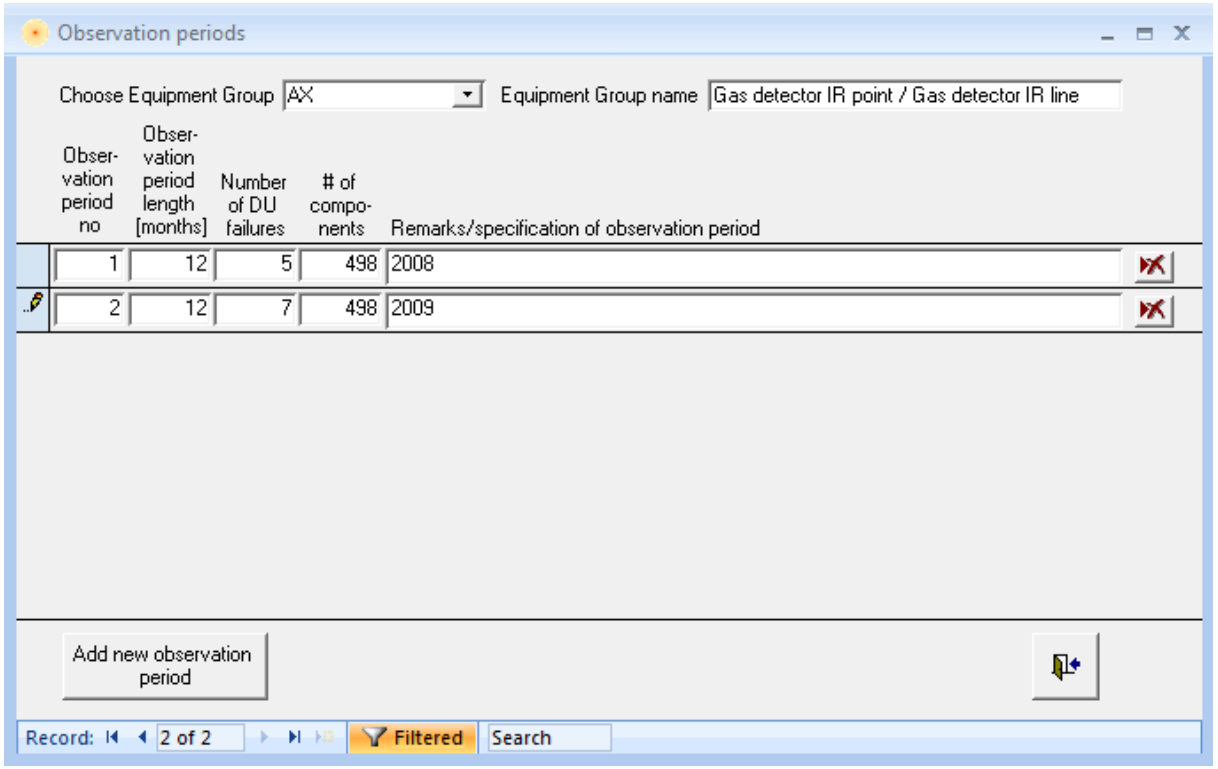
- Eksempler på CCF:
  - Temperatursvingninger påvirker hydraulikkoljen og gir gangtidsfeil
  - Feil valg av ventiler / ikke tilpasset bruk
  - Feil montering av ventiler/solenoider

PDS Tool – Operational follow up

- Operational follow up
  - estimate **updated failure rates** based on operational experience
  - evaluate the **possibility of changing the test interval** based on operational experience
  - **update the safety function calculations** with the new updated failure rates
- Definere utstyrsgrupper
- Legge inn observasjoner
- Oppdatere feildata
- Reporting: Follow-up report


Define Equipment Groups
Eq. Group ID
Component name
Element type
λDU,0 (/10^6 hrs)
λ DU-CE (/10^6 hrs)
# of compo-nents
Initial τ (months)
BM ESD push button Sensor 0,40 0,80 93 12
BX Flame detector Sensor 0,80 1,60 580 12
FZT Flow transmitter Sensor 0,60 1,20 19 12
AX Gas detector IR line Sensor 0,70 1,40 285 12
AX Gas detector IR point Sensor 0,60 1,20 213 12
Gas detector, catalytic Sensor 1,80 3,60 12
H2S detector Sensor 0,50 1,00 12
Heat detector Sensor 0,60 1,20 12
LZT Level (displace) transmitter Sensor 0,60 1,20 96 12
Pressure switch, conventional Sensor 2,00 4,00 12
PT Pressure transmitter Sensor 0,30 0,60 136 12
Proximity switch, inductive Sensor 3,00 6,00 12
BO Smoke detector Sensor 0,70 1,40 807 12
TT Temperature transmitter Sensor 0,30 0,60 95 12
Hardwired safety system - digital output Logic 0,03 0,06 12
Hardwired safety system - input Logic 0,04 0,08 12
Hardwired safety system - logic Logic 0,03 0,06 12
Industrial PLC - analog input Logic 0,70 1,40 12
Industrial PLC - CPU Logic 3,50 7,00 12
Industrial PLC - digital output Logic 0,70 1,40 12
Programmable safety system - analog ir Logic 0,16 0,32 12
Programmable safety system - CPU Logic 0,48 0,96 12
Programmable safety system - digital ou Logic 0,16 0,32 12
Blowdown valve incl. actuator (ex. pilot Final 2,10 4,20 12
Circuit breaker (large) Final 0,30 0,60 12
Control valve (frequently operated) Final 2,20 4,40 12
Control valve (shutdown service only) Final 3,50 7,00 12
Deluge valve (complete) Final 3,00 6,00 12
Reset all Equipment Group definitions
Hide components not defined within a group
Create defined Equipment Groups
Record: 14 of 36
Unfiltered
Search


Equipment Groups
Eq. Group ID
Equipment Group name
Element type
λ DU,0 (/10^6 hrs)
λ DU-CE (/10^6 hrs)
# of compo-nents
Initial τ (months)
AX Gas detector IR point / Gas detector IF Sensor 0,66 1,31 498 12
BM ESD push button Sensor 0,40 0,80 93 12
BO Smoke detector Sensor 0,70 1,40 807 12
BX Flame detector Sensor 0,80 1,60 580 12
FZT Flow transmitter Sensor 0,60 1,20 19 12
LZT Level (displace) transmitter Sensor 0,60 1,20 96 12
PT Pressure transmitter Sensor 0,30 0,60 136 12
TT Temperature transmitter Sensor 0,30 0,60 95 12
Record: 1 of 8
No Filter
Search


Observation periods
Choose Equipment Group
AX
Equipment Group name
Gas detector IR point / Gas detector IR line
Obser-vation period no
Obser-vation period length [months]
Number of DU failures
# of compo-nents
Remarks/specification of observation period
1
12
5
498
2008
2
12
7
498
2009
Add new observation period
Record:
2 of 2
Filtered
Search

PDS Tool - Updated Failure Rates

Sensor

ESD push button

Initial failure rate	Period no	Period length [months]	# components	# failures	Acc. time in service [hrs]	Updated failure rate	Remarks
4,00E-07							
	1	12	93	0	814680	3,02E-07	2008
	2	12	93	1	1629360	4,84E-07	2009

Flame detector

Initial failure rate	Period no	Period length [months]	# components	# failures	Acc. time in service [hrs]	Updated failure rate	Remarks
8,00E-07							
	1	12	580	4	5080800	7,90E-07	2008

Gas detector IR point / Gas detector IR line

Initial failure rate	Period no	Period length [months]	# components	# failures	Acc. time in service [hrs]	Updated failure rate	Remarks
6,57E-07							
	1	12	498	5	4362480	1,02E-06	2008
	2	12	498	7	8724960	1,27E-06	2009

Takk for oppmerksomheten!

www.sintef.no/sipaa

solfrid.habrekke@sintef.no